	(\$ FEB 0 1 2002 15)			
			Sheet 1 of 2	
ĺ	FORM PTO-1449 U.S. DEPARTMENT OF COMMERCE	ATTORNEY DOCKET NO.	APPLICATION NO.	
I	PATENT AND TRADEMARK OFFICE	1573.1010	10/028,265	
۱		FIRST NAMED INVENTOR		
١	LIST OF REFERENCES CITED BY APPLICANT	Koichi ITO, et al.		
I	(1)	FILING DATE	GROUP ART UNIT	
١	(Use several sheets if necessary)	December 28, 2001		

	DOCUMENT	U.S. PA	ATENT DOCUMENTS	1	SUB-	FILING
	NO.	DATE	NAME	CLASS	CLASS	DATE
AA						
AB	_					
AC	-					
	AB	AA AB	DOCUMENT NO. DATE AA AB	AA DATE NAME AB	AA AB DOCUMENT NO. DATE NAME CLASS	DOCUMENT NO. DATE NAME CLASS CLASS AA AB

FOREIGN PATENT DOCUMENTS SUB-TRANSLATION DOCUMENT CLASS NO. DATE COUNTRY CLASS YES NO AD 2000-305453 11/2000 Χ Japan ΑE WO 99/67919 12/1999 WIPO X 08/2000 WIPO X WO 00/46953 AF 05/2000 WIPO X AG WO 00/27068 $\overline{\mathsf{X}}$ ÁΗ WO 00/49765 08/2000 **WIPO** Х 02/2001 WIPO Αl WO 01/10077.

OTHER REFERENCES (Including Author, Title, Date, Pertinent Pages, Etc.)

AJ Kocker, Paul, et al., "Differential Power Analysis" in Proceedings of Advances in Cryptology-CRYPTO '99, Springer-Verlag 1999. pages 388-397.

AK Messerges, Thomas, et al., "Power Analysis Attacks of Modular Exponentiation in Smartcards", Cryptographic Hardware and Embedded Systems (CHES '99), Springer-Verlag, pages 144-157

AL Akkar, Mehdi-Laurent, et al., "Power Analysis, What is Now Possible...", ASIACRYPT 2000, Pages 489-502.

AM Messerges, Thomas S., "Securing the AES Finalists Against Power Analysis Attacks", Proceedings of Fast Software Encryption Workshop 2000, Springer-Verlag, April 2000, which is called "a masking method."

EXAMINER			DATE CONSIDERED	
John h	hopy !	1	10/4/05	<u></u>

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609; Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

Sheet 2 of 2

FEB 0 1 2002 FORM PTO-1449 LIST OF REFERENCES CITED BY APPLICANT

U.S. DEPARTMENT OF COMMERCE PATENT AND TRADEMARK OFFICE

(Use several sheets if necessary)

ATTORNEY DOCKET NO. 1573.1010

APPLICATION NO. 10/028,265

FIRST NAMED INVENTOR Koichi ITO, et al.

FILING DATE

December 28, 2001

GROUP ART UNIT

U.S. PATENT DOCUMENTS

U.S. FAILNI DOCUMENTO							
*EXAMINER INITIAL		DOCUMENT NO.	DATE	NAME	CLASS	SUB- CLASS	FILING DATE
	ВА						i
	ВВ				,		
	ВС						
	BD		·				
	BE						
	BF						

FOREIGN PATENT DOCUMENTS

		DOCUMENT NO.	DATE	COUNTRY	CLASS	SUB- CLASS	TRANS YES	LATION NO
1/MS	BG	WO 00/24155	04/2000	WIPO	-	(X	
1M5	вн	WO 00/24156	04/2000	WIPO	_		Х	
	ВІ							
	BJ							
	вк							
	BL							

OTHER REFERENCES (Including Author, Title, Date, Pertinent Pages, Etc.)

1M5	ВМ	Messerges, Thomas S. et al., "Investigations of Power Analysis Attacks on Smartcards", Proceedings of USENIX Workshop on Smartcard Technology, March 1999.
	BN	Chari, Suresh, et al., "A Cautionary Note Regarding Evaluation of AES Candidates on Smart-Cards", Second Advanced Encryption Standard Candidate Conference, March 1999.
	во	FIPS 46, "Data Encryption Standard" Federal Information Processing Standards Publication 46, U.S. Departement of Commerce/National Bureau of Standards, National Technical Information Service, Springfield, VA, 1977.
1	ВР	http://csrc.nist.gove/encryption/aes/rijndael/Rijndael.pdf (which is linked from http://www.nist.gov/aes/).

EXAMINER MAN	vi	DATE CONSIDERED	10/4/05
*EXAMINER: Initial if reference considered. w	hether of not citation i	s in conformance with MPEP 6	609: Draw line through citation if



Sheet 1 of 1 APPLICATION NO. ATTORNEY DOCKET NO. U.S. DEPARTMENT OF COMMERCE **FORM PTO-1449** PATENT AND TRADEMARK OFFICE 10/028,265 1573.1010 FIRST NAMED INVENTOR LIST OF REFERENCES CITED BY APPLICANT Koichi ITO, et al. FILING DATE GROUP ART UNIT (Use several sheets if necessary) 2131 December 28, 2001

	1	DOOLUGENT		ATENI DOCUMENTS		SUB-	FILING
*EXAMINER		DOCUMENT NO.	DATE	NAME	CLASS	CLASS	DATE
INITIAL	,	INO.	DATE	NAME	CLASS	02.00	DAIL
	AA	5,452,358	09/1995	Normile et al.			
	AB				REC	EIVED	
	AC				AUG	1 4 2003	
	AD				Technolog	y Center 210	00
1	AE						
	AF						

FOREIGN PATENT DOCUMENTS

TOREIGH FATERT BOOGINERTO								
		DOCUMENT NO.	DATE	COUNTRY	CLASS	SUB- CLASS	TRANSL YES	NO NO
7:00	AG	0 981 223 A2	02/2000	European Patent Office				
IMS	АН	0 792 041 A2	08/1997	European Patent Office		- /		
	Al							
	AJ							
	AK							
,	AL							

OTHER REFERENCES (Including Author, Title, Date, Pertinent Pages, Etc.)					
TMS AM	Messerges, Thomas S., "Securing the AES Finalists Against Power Analysis Attacks", PROCEEDINGS OF FAST SOFTWARE ENCRYPTION WORKSHOP 2000, April 10-20, 2000, pages 150-164.				

EXAMINER /		DATE CONSIDERED	_
CI had	, ,	100/4/ac	
Jan X/	Lund	10/1/03	
*FXAMINER: Initial if reference cons	iffered whether or not cita	tion is in conformance with MPEP 609.	Draw line through

citation if not in conformance and not considered. Include copy of this form with next communication to applicant.